ON ℓ-ADIC REPRESENTATIONS FOR A SPACE OF NONCONGRUENCE CUSPFORMS

JEROME WILLIAM HOFFMAN, LING LONG, AND HELENA VERRILL

Abstract. This paper is concerned with a compatible family of 4-dimensional ℓ-adic representations ρ_ℓ of $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ attached to the space of weight 3 cuspforms $S_3(\Gamma)$ on a noncongruence subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$. For this representation we prove that:

1. It is automorphic: the L-function $L(s, \rho_\ell^\vee)$ agrees with the L-function for an automorphic form for $\mathrm{GL}_4(\mathbb{A}_{\mathbb{Q}})$, where $\rho_\ell^\vee$ is the dual of ρ_ℓ.
2. For each prime $p \geq 5$ there is a basis $h_p = \{h_p^+, h_p^-\}$ of $S_3(\Gamma)$ whose expansion coefficients satisfy 3-term Atkin and Swinnerton-Dyer (ASD) relations, relative to the q-expansion coefficients of a newform f of level 432. The structure of this basis depends on the class of p modulo 12.

The key point is that the representation ρ_ℓ admits a quaternion multiplication structure in the sense of [ALLL10].

1. Introduction

1.1. Recall that a subgroup of finite index $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ is a congruence subgroup if $\Gamma \supset \Gamma(N)$ for some integer $N \geq 1$, where $\Gamma(N) \subset \mathrm{SL}_2(\mathbb{Z})$ is the normal subgroup consisting of matrices congruent to the identity modulo N; Γ is a noncongruence subgroup if it is not a congruence subgroup. There is a vast theory of modular forms on congruence subgroups (general reference for facts and notation: [Shi71], [DS05]). By contrast, modular forms on noncongruence subgroups are less well-understood, and they exhibit qualitatively different behavior. It is well known that $S_k(\Gamma_0(N), \chi)$ has a basis of Hecke eigenforms, which have q-expansions

$$f(z) = \sum_{n\geq 1} a_n(f) q^n, \quad \text{where} \quad q = \exp(2\pi i z),$$

with a_n satisfying the relations

$$a_{np} - a_p a_n + \chi(p) p^{k-1} a_{n/p} = 0, \quad a_n = a_n(f) \tag{1}$$

for all positive integers n and primes $p \nmid N$, taking $a_{n/p} = 0$ if $p \nmid n$. Moreover, a_p is the trace of Frobenius for a two-dimensional λ-adic representation ρ_f of $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ ([Del68, DS75, Lan72]).

Date: today.

The second author was supported in part by the NSA grant #H98230-08-1-0076. Part of the work was done during Long's visit to University of California at Santa Cruz. This research was initiated during an REU summer program at LSU, supported by the National Science Foundation grant DMS-0353722 and a Louisiana Board of Regents Enhancement grant, LEQSF (2002-2004)-ENH-TR-17. The last author was partially supported by grants LEQSF (2004-2007)-RD-A-16 and NSF award DMS-0501318.

1.2. If Γ is a noncongruence subgroup, there is in general no Hecke eigenbasis for $S_k(\Gamma)$, the space of weight k cuspforms for Γ, but rather it is conjectured that, at least in certain circumstances, for almost all primes p there is a basis $\{h_j = h_{p,j}\}$ such that the q-expansion coefficients satisfy 3-term Atkin-Swinnerton-Dyer (ASD) congruences in the general shape:

$$a_{np}(h_j) - \alpha_p(j)a_n(h_j) + \chi_j(p)p^{k-1}a_{n/p}(h_j) \equiv 0 \bmod (np)^{k-1} \tag{2}$$

where $|\alpha_p(j)| \leq 2p^{(k-1)/2}$ and $\chi_j(p)$ is a root of unity. In [Sch85i, Sch85ii], A. J. Scholl proved the existence of $(2d+1)$-term ASD congruences ($d = \dim S_k(\Gamma)$), under some standard assumptions such as the modular curve being defined over $\mathbb{Q}$ with infinity as a $\mathbb{Q}$-rational point. In fact, for every prime ℓ, Scholl proved the existence of a $G_{\mathbb{Q}}$-representation $\rho_\ell = \rho_{\Gamma,k,\ell}$ acting on an ℓ-adic space $W_\ell(\Gamma)$ of dimension $2d$ analogous to Deligne's construction for congruence subgroups. He also constructed $2d$-dimensional $\mathbb{Q}_p$-vector spaces, $V_p(\Gamma)$, with an action of a Frobenius operator and containing the subspace $S_k(\Gamma) \otimes \mathbb{Q}_p$, which are the analogs in crystalline cohomology of the ℓ-adic space $W_\ell(\Gamma)$. Scholl achieved the $(2d+1)$-term ASD congruences via a comparison theorem. He managed to refine this to obtain 3-term congruences when the characteristic polynomials of those $(2d+1)$-term recursions have d distinct p-adic roots. In special cases involving extra symmetries, such as 4-dimensional Scholl representations satisfying Quaternion Multiplications (see [ALLL10]), we can find in a systematic way a basis of the noncongruence modular forms whose members satisfy 3-term congruences, see Section 6.

In recent studies ([LLY05], [Lon08], [ALL08], [FHL+08], [ALLL10], to which we send the reader for more background and precise conjectures) the $\alpha_p(j)$, up to multiplying by roots of unity in clear patterns, are the pth q-expansion coefficients of newforms f_j on *congruence* subgroups. To be more precise, there is a quadratic field K such that $T^2 - a_p(j)T + \chi_j(p)p^{k-1}$ is the Hecke polynomial at some place of K over p for some automorphic form for GL_2 over K (see [ALLL10, Thm. 4.3.2] for details).

1.3. In this paper, we have a particular noncongruence group Γ and $k = 3$, $d = 2$. Experimentally it was discovered that the degree 4 polynomials of the geometric Frobenii under the corresponding Scholl representation (denoted by $\rho_{\ell,2}$ below) factor into quadratic pieces with coefficients in $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-6})$, respectively as p is congruent to 1 mod 3, 5 mod 12, or 11 mod 12, and moreover, the linear terms in these polynomials matched the pth Fourier coefficients of a newform f of level 432, up to multiplication by a twelfth root of unity. This trichotomy is explained by the existence of an order-8 quaternion group acting on $\rho_{\ell,2}$. This falls into the general framework of 4-dimensional Galois representations admitting quaternion multiplications that is studied in detail in [ALLL10], except that the action of the quaternion group is not defined over a quadratic or biquadratic field. To overcome the extra complication, we use an auxiliary 4-dimensional $G_{\mathbb{Q}}$ representation $\rho_{\ell,4}$, which is a 4-dimensional Galois representation admitting quaternion multiplication defined over a biquadratic field. The automorphy of $\rho_{\ell,4}$ is known due to [ALLL10]. It requires additional work to link $\rho_{\ell,4}$ to the level 432 newform f. We use ρ_f to denote the 2-dimensional Deligne representation of $G_{\mathbb{Q}}$ attached to the Hecke newform f. The relations between $\rho_{\ell,2}$, $\rho_{\ell,4}$, and ρ_f are depicted by the following diagram. For the precise statements, see Corollary 1, Theorems 1, 2, and 3.

$$\begin{tikzcd}
\rho_{\ell,2} \arrow[rr, dash, dashed] \arrow[d, equal] \arrow[dr, dash, dashed] & & \rho_f \arrow[dl, dash, dashed] \arrow[d, dash, dashed] \\
\mathrm{Ind}_{G_{\mathbb{Q}(\sqrt{-3})}}^{G_{\mathbb{Q}}} \sigma_{\lambda,2,-3} \arrow[d, dash, dashed] & \rho_{\ell,4} = \mathrm{Ind}_{G_{\mathbb{Q}(\sqrt{-3})}}^{G_{\mathbb{Q}}} \sigma_{\lambda,4,-3} \arrow[dl, dash, dashed] \arrow[d, equal] & \mathrm{Ind}_{G_{\mathbb{Q}(i)}}^{G_{\mathbb{Q}}} [(\rho_f \mid_{G_{\mathbb{Q}(i)}}) \otimes \chi] \arrow[d, equal] \\
\sigma_{\lambda,4,-3} = \sigma_{\lambda,2,-3} \otimes \psi & \mathrm{Ind}_{G_{\mathbb{Q}(i)}}^{G_{\mathbb{Q}}} \sigma_{\lambda,4,-1} \arrow[r, dash, dashed] & (\sigma_{\lambda,4,-1})^{ss}
\end{tikzcd}$$

For a number field K, let G_K denote $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$. In the diagram above, both $\sigma_{\lambda,2,-3}$ and $\sigma_{\lambda,4,-3}$ are 2-dimensional representations of $G_{\mathbb{Q}(\sqrt{-3})}$, ψ is a cubic character of $G_{\mathbb{Q}(\sqrt{-3})}$ and χ is a quartic character of $G_{\mathbb{Q}(i)}$ where $i = \sqrt{-1}$.

1.4. For each prime $p \geq 5$ we prove that there exists a basis $h_p = \{h_p^+, h_p^-\}$ of $S_3(\Gamma)$ whose expansion coefficients satisfy 3-term Atkin and Swinnerton-Dyer (ASD) relations. To be more precise, there exists a finite extension E of $\mathbb{Q}_p$ such that the coefficients of $h_p^{\pm} = \sum_{n\geq 1} a_{\pm}(n)q^n \in \mathcal{O}_E[[q]]$ satisfy

$$a_{\pm}(np^r) - A_{p,\pm}a_{\pm}(np^{r-1}) + B_{p,\pm}a_{\pm}(np^{r-2}) \equiv 0 \mod p^{r(k-1)}, \forall n, r \geq 1,$$

where $\mathcal{O}_E$ is the ring of integers of E, $A_{p,\pm}, B_{p,\pm} \in \mathcal{O}_E$ and the weight $k = 3$. We say that we have ASD congruences relative to the polynomial $X^2 - A_{p,\pm}X + B_{p,\pm}$. The structure of h_p depends only on the class of p mod 12. As an application of the modularity result mentioned above, $A_{p,\pm}, B_{p,\pm}$ are determined by the p-coefficient of f and the characters ψ and χ. See Propositions 4, 5, and 6.

1.5. The paper is organized as follows. In §2, we describe the group Γ and the family of elliptic curves $E(\Gamma) \to X(\Gamma)$ associated to it. In §3 we define some correspondences B_j of the elliptic surface $E(\Gamma)$. The main point is that these define a quaternion multiplication structure on associated cohomology spaces. In §4 we show that the 4-dimensional ℓ-adic representations $\rho_{\ell,2}$, $\rho_{\ell,4}$ are induced in several ways from subgroups of index two in $G_{\mathbb{Q}}$. §5 proves the main modularity theorem: the L-function of the representations $\rho_{\ell,2}^{\vee}$ (resp. $\rho_{\ell,4}^{\vee}$) can be expressed in terms of the Hecke L-function of a newform f of level 432 and some explicit characters. This is done by the method of Faltings-Serre. The ASD congruences are proved in §6. Tables of experimental data which form the basis of this paper appear in §7. These computations began in an REU project in summer 2005. The software systems `Magma`, `Mathematica`, and `pari/gp` were used.

2. The group and the space of noncongruence cuspforms

2.1. If $\Gamma_0 \subset \mathrm{SL}_2(\mathbb{Z})$ is a torsion-free subgroup of finite index we let $Y(\Gamma_0) = \Gamma_0\backslash\mathfrak{H}$ be the quotient of the upper half plane of complex numbers, and $j : Y(\Gamma_0) \to X(\Gamma_0)$ be the compactification by adding cusps. It is known that these are the $\mathbb{C}$-points of algebraic curves defined over number fields; in this paper, they will have models over $\mathbb{Q}$, which we will denote by the same symbols. Define the analytic space $E(\Gamma_0)$ as the quotient of $\mathbb{C} \times \mathfrak{H}$ by the equivalence relation

$$(z, \tau) \sim \left(\frac{z + m\tau + n}{c\tau + d}, \frac{a\tau + b}{c\tau + d}\right), \quad m, n \in \mathbb{Z}, \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0.$$

Then $f : E(\Gamma_0) \to Y(\Gamma_0)$ is a fibration of elliptic curves. When Γ_0 is a congruence subgroup, these are the $\mathbb{C}$-points of schemes defined over number fields and represent (at least coarsely) moduli problems for elliptic curves. In this paper, they will be defined over $\mathbb{Q}$ and designated by the same symbols.

2.2. (For generalities on the moduli spaces of elliptic curves, see [DeRa], [KM85]). The stack $[\Gamma_0(8)]$ classifies pairs (E, C) of elliptic curves E together with subgroup schemes $C \subset E$ locally isomorphic to $\mathbb{Z}/8$. Since $\pm 1 \in \Gamma_0(8)$ the map $[\Gamma_0(8)] \to M(\Gamma_0(8))$ is two to one, where for a congruence subgroup Γ_0, $M(\Gamma_0)$ denotes the corresponding (coarse) moduli scheme. One knows that $M(\Gamma_0(8)) \otimes \mathbb{Q} \cong \mathbf{P}^1_{\mathbb{Q}} = X(\Gamma_0(8))$.

2.3. The stack $[\Gamma_1(4)]$ classifies pairs (E, P) of elliptic curves E together with a point P of exact order 4. This time $[\Gamma_1(4)] = M(\Gamma_1(4))$. One knows that there are two connected components defined over $\mathbb{Q}(i)$ each of which is isomorphic to $\mathbf{P}^1_{\mathbb{Q}(i)}$.

2.4. The stack $[\Gamma_0(8) \cap \Gamma_1(4)]$ classifies triplets (E, C, P) of elliptic curves E together with $P \in C$ a point of exact order 4 in a cyclic subgroup of order 8. We have $[\Gamma_0(8) \cap \Gamma_1(4)] = M(\Gamma_0(8) \cap \Gamma_1(4))$. In fact, projectively $\pm\Gamma_0(8)/\pm I_2 = \pm(\Gamma_0(8) \cap \Gamma_1(4))/\pm I_2$ so the modular curves are the same: $M(\Gamma_0(8) \cap \Gamma_1(4)) \otimes \mathbb{Q} = M(\Gamma_0(8)) \otimes \mathbb{Q} \cong \mathbf{P}^1_{\mathbb{Q}}$. It has a fine moduli interpretation as the moduli space of triples (E, C, P) where E is an elliptic curve, $C \subset E$ is a subgroup scheme of order 8, and $P \in E$ is a point of order 4. A model for its universal elliptic curve is

$$E_8(t): \quad y^2 + 4xy + 4t^2y = x^3 + t^2x^2, \tag{3}$$

where $t = \frac{\eta(z)^8\eta(4z)^4}{\eta(2z)^{12}} = 1 - 8q + 32q^2 + \cdots \in \mathbb{Z}[[q]], q = e^{2\pi i z}$ cf. [FHL$^+$08]. The modular function t is a Hauptmodul of $\Gamma_0(8) \cap \Gamma_1(4)$: a generator of the function field of the modular curve. Let Γ be a special index 3 normal subgroup of $\Gamma_0 := \Gamma_0(8) \cap \Gamma_1(4)$ whose modular curve $X(\Gamma)$ is a cubic cover of $X(\Gamma_0(8) \cap \Gamma_1(4))$ unramified everywhere except the cusps $\frac{1}{2}$ and $\frac{1}{4}$ (whose t-values are ∞ and -1 respectively), with ramification degree 3. It is easy to see that the genus of $X(\Gamma)$ is also 0. To facilitate our calculation, we need to find an algebraic map between the two modular curves, in other words, we need to describe a relation between a Hauptmodul r_a of Γ and t. By our construction, $ar_a^3 = t + 1$ for some nonzero constant a. Here a is a rational number written in lowest form. As we look for a model so that the q-expansion of r_a is in a number field as small as possible, we take $a = 2$ in which case the coefficients of r_a can be chosen in $\mathbb{Q}$. The Riemann surface $Y(\Gamma) := \Gamma\backslash\mathfrak{H}$ has the structure of an algebraic curve over $\mathbb{Q}$. This group Γ is labeled by $\Gamma_{8^3\cdot6\cdot3\cdot1^3}$ in [FHL$^+$08]. The cusp widths of Γ are 8-8-8-6-3-1-1-1 from which we know Γ is a noncongruence subgroup. The quotient Γ_0/Γ is generated by $\zeta\Gamma$, where $\zeta = \begin{pmatrix} 5 & -2 \\ 8 & -3 \end{pmatrix}$. The matrix $A = \begin{pmatrix} 0 & -1 \\ 8 & 0 \end{pmatrix}$ normalizes Γ. Both matrices ζ and A induce actions on $X(\Gamma)$ as well as the spaces of cuspforms for Γ.

2.5. Note that in [FHL$^+$08], different choices of a are picked. The reason for varying a is that for some choices, the operators to be defined below had smaller fields of definition, whereas for other choices, the Galois representation corresponding to $S_3(\Gamma)$ and parameter a (see §4) was easier to analyze. Only two choices $a = 2, 4$ are relevant to this paper; the corresponding Hauptmoduls are denoted r_2 and r_4. We

let $f_a : E(\Gamma) \to Y(\Gamma)$ be the pull-back of the universal elliptic curve in the previous section via the covering of degree three:

$$\begin{array}{rcl} Y(\Gamma) & \to & Y(\Gamma_0(8) \cap \Gamma_1(4)) \\ r_a & \mapsto & ar_a^3 - 1 \end{array}$$

We let $\mathcal{E}_\Gamma$ be the complex elliptic surface obtained by completing and desingularizing $f : E(\Gamma) \to Y(\Gamma)$ over the compact curve $X(\Gamma) := (\Gamma\backslash\mathfrak{H})^*$, which is independent of the choice of a. The nonzero Hodge numbers of this surface are $h^{0,0} = h^{2,2} = 1$, $h^{1,1} = 30$, $h^{2,0} = h^{0,2} = 2$. In particular the space of weight three cuspforms

$$S_3(\Gamma) = H^0(\Omega^2_{\mathcal{E}_\Gamma/\mathbb{C}})$$

is two dimensional. This $S_3(\Gamma)$ has a basis (see [FHL$^+$08]):

(4)

$$h_1 = \sqrt[3]{H_1},\ H_1 := \frac{\eta(z)^4\eta(2z)^{10}\eta(8z)^8}{\eta(4z)^4}, \quad h_2 = \sqrt[3]{H_2},\ H_2 := \frac{\eta(z)^8\eta(4z)^{10}\eta(8z)^4}{\eta(2z)^4}.$$

3. Correspondences

3.1. Given two subgroups of finite index $\Gamma_1, \Gamma_2 \subset \mathrm{SL}_2(\mathbb{Z})$ and an element $\alpha \in \mathrm{M}_2(\mathbb{Z})$ with $\det(\alpha) > 0$ the double coset $\Gamma_1\alpha\Gamma_2$ determines a correspondence $\Gamma_2\backslash\mathfrak{H} \longrightarrow \Gamma_1\backslash\mathfrak{H}$. Namely, we have a diagram

$$\Gamma_2\backslash\mathfrak{H} \leftarrow \Gamma\backslash\mathfrak{H} \to \Gamma_1\backslash\mathfrak{H}$$

where $\Gamma = \Gamma_2 \cap \alpha^{-1}\Gamma_1\alpha$. The first arrow sends $\tau \in \mathfrak{H}$ to τ and the second arrow sends τ to $\alpha.\tau$. If Γ_2 is decomposed into cosets for the subgroup Γ

$$\Gamma_2 = \coprod_{i=1}^{d} \Gamma.\varepsilon_i,$$

so that the $\varepsilon_i.\tau$ are the elements of $\Gamma\backslash\mathfrak{H}$ projecting to $\tau \in \Gamma_2\backslash\mathfrak{H}$, then the double coset decomposes as

$$\Gamma_1\alpha\Gamma_2 = \coprod_{i=1}^{d} \Gamma_1.\alpha\varepsilon_i := \coprod_{i=1}^{d} \Gamma_1.\alpha_i$$

and the correspondence sends the point τ mod Γ_2 to the cycle

$$\sum_{i=1}^{d} \alpha_i\tau \bmod \Gamma_1.$$

3.2. This diagram lifts to morphisms

$$E(\Gamma_2) \overset{p_2}{\leftarrow} E(\Gamma) \overset{p_1}{\rightarrow} E(\Gamma_1)$$

The arrow on the left is induced by $(z, \tau) \to (z, \tau)$. This is a fiberwise isomorphism. The map on the right is induced from

$$(z, \tau) \mapsto (\det(\alpha).z/j(\alpha, \tau), \alpha.\tau).$$

This is a fiberwise isogeny.

3.3. The double coset $\Gamma_1\gamma\Gamma_2$ induces maps on cohomology via

$$p_{2*}\circ p_1^*: H^i(\mathcal{E}^k_{\Gamma_1},\mathbb{Q})\to H^i(\mathcal{E}^k_{\Gamma_2},\mathbb{Q})$$

for any integer $k\geq 1$, where $\mathcal{E}^k_\Gamma$ denotes the desingularization of the k-fold fiber product of $\mathcal{E}_\Gamma/X(\Gamma)$. Recall that there is a canonical injection $S_{k+2}(\Gamma)\hookrightarrow H^1(\mathcal{E}^k_\Gamma,\mathbb{C})$ for $k\geq 1$ which identifies it with the $(k+1,0)$ part of the Hodge structure of pure weight on the right-hand side. The induced map given by the double coset $S_{k+2}(\Gamma_1)\to S_{k+2}(\Gamma_2)$ is given by the slash operator:

$$f\mid[\Gamma_1\alpha\Gamma_2]_{k+2}=\det(\alpha)^{k/2}\sum_{i=1}^{d} f\mid[\alpha_i]_{k+2}$$

see [Shi71, Ch. 3, especially 3.4].

3.4. We apply the above to the group $\Gamma_1=\Gamma_2=\Gamma_0(8)$ and the matrix

$$\alpha=A=\begin{pmatrix}0&-1\\8&0\end{pmatrix}$$

which normalizes $\Gamma_0(8)$. Then $k=1$, $d=1$ and $\alpha_1=\alpha$, $p_2=\mathrm{id}$ so that the map on cohomology is given by p_1^*. The involution of the modular curve $Y(\Gamma_0(8))$ induced by this matrix has the moduli interpretation $(E,C)\mapsto(E/C,E[8]/C)$, where $(E,C)\in Y(\Gamma_0(8))$ is an elliptic curve with a cyclic subgroup of order 8, and $E[8]$ is the kernel of multiplication by 8. Recall that t was our chosen Hauptmodul for the curve $Y(\Gamma_0(8))$. By a direct calculation, we know $A=\begin{pmatrix}0&-1\\8&0\end{pmatrix}$ induces the following map on $X(\Gamma_0(8)\cap\Gamma_1(4))$ (see [FHL+08]):

$$t\mapsto\frac{1-t}{1+t}. \tag{5}$$

In this case, the map p_1^* factors

$$E_8(t)\xrightarrow{A'}A^*E_8(t)=E_8\left(\frac{1-t}{1+t}\right)\xrightarrow{A''}E_8(t).$$

Here A'' is an isomorphism defined over $\mathbb{Q}$, because it is the base-change along $E(\Gamma_0(8))\to Y(\Gamma_0(8))$ of the involution A of $Y(\Gamma_0(8))$, which is an isomorphism defined over $\mathbb{Q}$. Then p_1^* is an isogeny defined over $\mathbb{Q}(i)$ covering the automorphism of $\mathbb{Q}(t)$ given by A because of:

Proposition 1. *This action of A on $X(\Gamma_0(8)\cap\Gamma_1(4))$ lifts to an isogeny A' : $E_8(t)\to E_8\left(\frac{1-t}{1+t}\right)$ defined over $\mathbb{Q}(i,t)$.*

Proof. It can be shown that there is no isogeny $E_8(t)\to E_8(\frac{1-t}{1+t})$ defined over $\mathbb{Q}(t)$. One way to see this is by specializing t to have rational values. These calculations were carried out using Magma and Mathematica. First one calculates the quotient curve $E_8(t)/C$ where C the universal subscheme giving the cyclic group of order 8. This is the subgroup scheme defined by $(x^2-4tx-4t^3)(x+t^2)x=0$. This gives the curve $E_8'(t): y^2+4xy+4t^2y=x^3+t^2x^2+b(t)x+c(t)$, where $b(t)=-5t^4-320t^3-720t^2-320t$, and $c(t)=3t^6-704t^5-5184t^4-8896t^3-5888t^2-1024t$, and an explicit isogeny $\psi: E_8(t)\to E_8'(t)$ defined over $\mathbb{Q}(t)$. Next one constructs an isomorphism $\phi: E_8'(t)\to E_8(\frac{1-t}{1+t})$. It is

$$(x,y)\mapsto(\phi_1(x,y),\phi_2(x,y))$$

where

$$\phi_1(x,y) = -\frac{7t^2+8t+x+8}{4(t+1)^2},$$
$$\phi_2(x,y) = \frac{12t^3+2(i+38)t^2+4(x+20)t+2(i+2)x+iy+16}{8(t+1)^3}.$$

The isogeny is $\phi\circ\psi$. More explicitly, we can write $\psi = \psi'''\circ\psi''\circ\psi'$ where

$$\psi_1'(x,y) = \frac{t^4+xt^2+x^2}{t^2+x}, \quad \psi_2'(x,y) = \frac{-4t^6-4xt^4+2xyt^2+x^2y}{(t^2+x)^2}$$
$$\psi_1''(x,y) = \frac{t^2(x-16)-x^2}{t^2-x}, \quad \psi_2''(x,y) = \frac{yt^4-2(8y+x(y+32))t^2+x^2y}{(t^2-x)^2},$$
$$\psi_1'''(x,y) = \frac{-64t^3+(x-128)t^2+8(x-8)t-x^2}{t^2+8t-x}$$
$$\psi_2'''(x,y) = \frac{P(x,y)}{(t^2+8t-x)^2},$$

$P(x,y) = (y+1024)t^4 - 16(16x+3y-128)t^3 - 2(32(y-16)+x(y+256))t^2 - 16(4y+x(y+16))t + x^2y.$ □

3.5. The involution A of the modular curve $X(\Gamma_0(8)\cap\Gamma_1(4))$ lifts to an involution of the curve $X(\Gamma)$ where $\Gamma\subset\Gamma_0(8)\cap\Gamma_1(4)$ is defined in §2.4. Let r_4 be the Hauptmodul for this curve with $t = 4r_4^3-1$. Under the action of A, $r_4\mapsto 1/2r_4$. By base-change, the isogeny A defined in the above proposition lifts to an isogeny of the elliptic curve $E(\Gamma)$, which we will denote by $E(r_4)$. This map defined over $\mathbb{Q}(i)$. For the purposes of the ASD congruences, we need that the curve $X(\Gamma)$ has a $\mathbb{Q}$-rational cusp corresponding to $\tau = i\infty$; unfortunately, this is not the case for this model: the point $\tau = i\infty$ corresponds to $t=1$ and there is no $\mathbb{Q}$ -rational r_4 with $t = 1 = 4r_4^3-1$. In the model with $t = 2r_2^3-1$ corresponding to the representation $\rho_{\ell,2}$ (details see §4), there is a $\mathbb{Q}$-rational point over $t=1$, namely $r_2 = 1$. But in this model, the involution A is now given by $r_2\mapsto 1/\sqrt[3]{2}r_2$, and this gives an isogeny of $E(\Gamma)$ defined over the larger field $\mathbb{Q}(i,\sqrt[3]{2})$. In either of these models, ζ acts on the Hauptmodul by $r_a\mapsto \exp(2\pi i/3)\, r_a$.

3.6. On the p-adic space V_p (see sections 1.2 and 6.1), we define operators

$$B_{-1} = A, \quad B_{-3} = \zeta-\zeta^2, \quad B_3 = A(\zeta-\zeta^2),$$

where A and ζ are given in §2.4.

Proposition 2. *$B_{-1}^2 = -8$; $B_{-3}^2 = -3$; $B_3^2 = -24$; $B_{-1}B_{-3} = -B_{-3}B_{-1}$.*

Proof. To prove the identities, it suffices to prove them for the corresponding operators on $S_3(\Gamma)$. The reason is that this is the Hodge $(2,0)$ component of $H_{DR}({}^3_\Gamma\mathcal{W})$ for Scholl's motive (see [Sch90]), these operators act on this motive, which is a natural factor of $H^2(\mathcal{E}_\Gamma)$, and $V_p = H_{cris}({}^3_\Gamma\mathcal{W})$. [1] The effect of ζ on the basis h_1, h_2

[1]Scholl only constructs ${}^k_n\mathcal{W}$ for principal congruence subgroups of level n. But the construction also works here: it is the Grothendieck motive which is formal image of the projector denoted Π_ε in loc. cit. acting on the elliptic surface $\mathcal{E}_{\Gamma,a}$, now regarded as a scheme over $\mathbb{Q}$.

(see (4)) is given by the matrix

$$\zeta := \begin{pmatrix} \omega_3 & 0 \\ 0 & \omega_3^{-1} \end{pmatrix}$$

where ω_3 is a primitive cubic root of unity. To compute the effect of A we use the stroke operator defined in section (3.3) on $H_1 = h_1^3$, $H_2 = h_2^3$, and use properties of the η-function. The result is, in the basis h_1, h_2

$$A := \begin{pmatrix} 0 & i2^{4/3} \\ i2^{5/3} & 0 \end{pmatrix}$$

These identities follow immediately. □

4. ℓ-adic representations

In this paper, for any place v of a number field K, we use Fr_v and $\mathrm{Frob}_v := \mathrm{Fr}_v^{-1}$ to denote the corresponding arithmetic Frobenius and geometric Frobenius, respectively. We use ℓ to denote an arbitrary prime, unless it is specified.

4.1. If $j : Y(\Gamma) \to X(\Gamma)$ is the inclusion, we define

$$W_{\ell,a} = H^1(X(\Gamma) \otimes \overline{\mathbb{Q}},\ j_* R^1 f_{a*} \mathbb{Q}_\ell)$$

which is a 4-dimensional $\mathbb{Q}_\ell$-space, where étale cohomology is understood, and we are using the symbols $Y(\Gamma)$ and $X(\Gamma)$ to denote the schemes over $\mathbb{Q}$ whose $\mathbb{C}$-valued points were previously denoted by these letters. We thus obtain a continuous ℓ-adic representation

$$\rho_{\ell,a} : G_{\mathbb{Q}} \to \mathrm{GL}(W_{\ell,a}) = \mathrm{GL}_4(\mathbb{Q}_\ell).$$

Let $N(a)$ be the least common multiple of the numerator and denominator of a. This representation is unramified outside of $2, 3, \ell, N(a)$, and for all primes $p \nmid 6\ell N(a)$, we have the characteristic polynomial of Frobenius

$$\det(X - \rho_{\ell,a}(\mathrm{Frob}_p)) = \mathrm{Char}(\mathrm{Frob}_p, W_{\ell,a}, X) = H_{p,a}(X) \in \mathbb{Z}[X].$$

A useful fact is that the roots of $H_{p,a}(X)$ have the same absolute value (cf. [Sch85ii]), which is p in this case.

4.2. When $a = 4$, it was first observed experimentally that there are factorizations

$$H_{p,4}(X) = g_{p,4}(X)\overline{g_{p,4}(X)},$$

where the bar notation stands for complex conjugation and the coefficients of the quadratic polynomials $g_{p,4}(X)$ lie respectively in the fields $\mathbb{Q}$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-6})$ as $p \equiv 1, 7, 5, 11 \bmod 12$. This is a property that follows from $\rho_{\ell,4}$ satisfying the so-called quaternion multiplication over the biquadratic field $\mathbb{Q}(\sqrt{-3}, \sqrt{-2})$ in the sense of [ALLL10, §3]. To be more precise, we consider the following maps on $W_{\ell,4} \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell$. Let ζ^* be the map on $W_{\ell,4}$ induced by ζ and A^* be the map induced by A (see §3.4 and a related discussion in [ALLL10, §5]). It sends $E(\Gamma)$ to an isogenous elliptic curve over $\mathbb{Q}(i, r_4)$. It is obvious that ζ^* is defined over $\mathbb{Q}(\sqrt{-3})$. By §3.4, A^* is defined over $\mathbb{Q}(i)$. We define the following operators on $W_{\ell,4} \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell$: $B_{-1}^* = A^*, B_{-3}^* = \zeta^* - (\zeta^*)^2$; as well as

$$J_{-1} = \frac{1}{\sqrt{8}} B_{-1}^*, \quad J_{-3} = \frac{1}{\sqrt{3}} B_{-3}^*, \quad J_3 = J_{-1} J_{-3}$$

These depend on choices of embeddings $\sqrt{8}, \sqrt{3} \in \overline{\mathbb{Q}}_\ell$, but the decompositions that follow below do not depend on these choices.

Proposition 3. *1. $J_{-1}^2 = -1$; $J_{-3}^2 = -1$; $J_{-1}J_{-3} = -J_{-3}J_{-1}$.*

2. When $a = 4$, for $s \in \{-1, -3, 3\}$, $J_s\rho_{\ell,4} = \varepsilon_s\rho_{\ell,4}J_s$ where $\varepsilon_s : G_{\mathbb{Q}} \to \mathbb{C}^*$ is the quadratic character of $G_{\mathbb{Q}}$ whose kernel is $G_{\mathbb{Q}(\sqrt{s})}$.

Proof. (1) In the proof of Proposition 2 these identities were shown to hold on $H_{DR}({}^3_\Gamma\mathcal{W})$. By comparison isomorphisms, these also hold on $H_\ell({}^3_\Gamma\mathcal{W}) = W_{\ell,a}$.

(2) The Galois group $G_{\mathbb{Q}}$ interacts with the operators $J_{\pm 3}, J_{-1}$ in the same way that it interacts with the $B_{-1}^*, B_{-3}^*, B_3^*$, in other words the irrationalities $\sqrt{8}, \sqrt{3}$ do not affect the Galois action: the reason is that one treats the second factor in $W_{\ell,4} \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell$ as the trivial Galois module. Thus, when $a = 4$, by the discussion right before the proposition, $\mathbb{Q}(i)$ (resp. $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{3})$) is the minimal field of definition of J_{-1} (resp. J_{-3}, J_3). Thus the commutativity of $G_{\mathbb{Q}}$ and J_{-1}, J_{-3}, J_3 is as claimed. □

Corollary 1. *1. Let $D_{-1} = -2$, $D_{-3} = -3$, $D_3 = -6$. For each $s \in \{-1, -3, 3\}$, let $K_s = \mathbb{Q}(\sqrt{D_s})$ and λ be the place of $\mathbb{Q}_\ell(\sqrt{D_s}) = K_{s,\lambda}$ lying over ℓ. Then*

$$\rho_{\ell,4} \otimes_{\mathbb{Q}_\ell} K_{s,\lambda} = \mathrm{Ind}_{G_{\mathbb{Q}(\sqrt{s})}}^{G_{\mathbb{Q}}}(\sigma_{\lambda,4,s}), \tag{6}$$

for some 2-dimensional absolutely irreducible representation $\sigma_{\lambda,4,s}$ of $G_{\mathbb{Q}(\sqrt{s})}$.

2. The determinant $\det \sigma_{\lambda,4,s} = \varphi_s \cdot (\epsilon_\ell|_{G_{\mathbb{Q}(\sqrt{s})}})^2$ where ϵ_ℓ is the ℓ-adic cyclotomic character and φ_s is the quadratic character of $G_{\mathbb{Q}(\sqrt{s})}$ with kernel $G_{\mathbb{Q}(i,\sqrt{3})}$.

Proof. 1. For each s the eigenspaces of B_s^* are each two dimensional, defined over K_s, invariant under $G_{\mathbb{Q}(\sqrt{s})}$. Thus $\rho_{\ell,4} \otimes_{\mathbb{Q}_\ell} K_{s,\lambda}|_{G_{K_s}} = \sigma_{\lambda,4,s} \oplus \sigma'_{\lambda,4,s}$ where $\sigma_{\lambda,4,s}$ and its conjugate $\sigma'_{\lambda,4,s}$ are 2-dimensional. It is straightforward to check, by using the data listed in Table 2, they are absolutely irreducible and non-isomorphic. Thus (6) follows from Clifford's result in [Cli37]. Moreover, by [Cli37] one knows $\sigma_{\lambda,4,s} = \sigma'_{\lambda,4,s} \otimes \chi_s$ where χ_s is the quadratic character of $G_{\mathbb{Q}}$ with fixed field K_s.

2. By a direct calculation, one knows that $\det \rho_{\ell,4} = \epsilon_\ell^4$. It follows from $\sigma_{\lambda,4,s} = \sigma'_{\lambda,4,s} \otimes \chi_s$ that $\det \sigma_{\lambda,4,s} = \varphi_s \cdot (\epsilon_\ell|_{G_{\mathbb{Q}(\sqrt{s})}})^2$ for some character φ_s of $G_{\mathbb{Q}(\sqrt{s})}$ of order at most 2. From the data (Table 2) and the fact that φ_s only ramifies at places of $\mathbb{Q}(\sqrt{s})$ above 2 and 3, we can conclude that the fixed field of φ_s is $G_{\mathbb{Q}(i,\sqrt{3})}$. □

Theorem 1. *1. The semi-simplification of $\rho_{\ell,4}^\vee$, the dual of $\rho_{\ell,4}$, is automorphic, i.e. the L-function of $\rho_{\ell,4}^\vee$ is equal to the L-function of an automorphic representation of $GL_4(\mathbb{A}_{\mathbb{Q}})$.*

2. To be more precise, $L(s, \rho_{\ell,4}^\vee) = L(s, (\rho_f|_{G_{\mathbb{Q}(i)}}) \otimes \chi)$ for some level 432 Hecke newform f and some quartic character χ of $G_{\mathbb{Q}(i)}$.

The first claim follows from 4.2.4 and 4.2.5 of [ALLL10]. We will postpone the proof of the second claim to the next section. See Theorem 3.

4.3. When $a = 2$, the operator B_{-3}^* on $\rho_{\ell,2}$ is defined over $\mathbb{Q}(\sqrt{-3})$. Because of it, $\rho_{\ell,2} \otimes_{\mathbb{Q}_\ell} K_{-3,\lambda}$ is also induced from a 2-dimensional representation $\sigma_{\lambda,2,-3}$ of $G_{\mathbb{Q}(\sqrt{-3})}$ (see [Lon08]). The factorization of $H_{p,2}(X)$ is given in Table 1.

Theorem 2. *Let K be the splitting field of x^3-2 over $\mathbb{Q}$. Then $\sigma_{\lambda,4,-3} = \sigma_{\lambda,2,-3} \otimes \psi$ where ψ is a cubic character of $G_{\mathbb{Q}(\sqrt{-3})}$ with kernel G_K.*

Proof. Note that $\rho_{\ell,2}\mid_{G_K}$ and $\rho_{\ell,4}\mid_{G_K}$ are isomorphic as the corresponding elliptic modular surfaces become isomorphic over K. It is routine to check that $\sigma_{\lambda,2,-3}\mid_{G_K}$ and $\sigma_{\lambda,4,-3}\mid_{G_K}$ are absolutely irreducible. Upon replacing $\sigma_{\lambda,2,-3}$ by its conjugate under any element in $G_{\mathbb{Q}}\setminus G_{\mathbb{Q}(\sqrt{-3})}$, we may assume that

$$\sigma_{\lambda,2,-3}|_{G_K}=\sigma_{\lambda,4,-3}|_{G_K}.$$

By Theorem 5 of [Cli37], $\sigma_{\lambda,2,-3}$ and $\sigma_{\lambda,4,-3}$ are either isomorphic or differ by a cubic character ψ of $G_{\mathbb{Q}(\sqrt{-3})}$ with kernel G_K. Numerical data in Tables 1 and 2 reveal that they are not isomorphic. $\square$

Lemma 1. *For any prime $p\equiv 2 \mod 3$ (which is inert in $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$), $\psi(p)=1$.*

Proof. The polynomial X^3-2 has exactly one root in $\mathbb{F}_p$ when $p\equiv 2 \mod 3$ as $X\mapsto X^3$ is a bijection in $\mathbb{F}_p$. Thus for any prime $p\equiv 2 \mod 3$, which is inert in $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$, it splits completely in the Galois extension K of $\mathbb{Q}(\sqrt{-3})$. This means $\psi(p)=1$. $\square$

5. Modularity

Our goal is to prove Theorem 1. Since $\rho_{\ell,4}$ satisfies quaternion multiplication over $\mathbb{Q}(i,\sqrt{-3})$, by the main result of [ALLL10] the L-function of $\rho_{\ell,4}^\vee$ coincides with the L-function of a $\mathrm{GL}_4(\mathbb{A}_{\mathbb{Q}})$ automorphic form. Here we will prove this claim directly. [2]

We identified using William Stein's Magma package the following Hecke eigenform

$$\begin{aligned} f(z) &= q+6\sqrt{2}q^5+\sqrt{-3}q^7+6\sqrt{-6}q^{11}+13q^{13}-6\sqrt{2}q^{17}+11\sqrt{-3}q^{19}\\ &\quad -18\sqrt{-6}q^{23}+47q^{25}-24\sqrt{2}q^{29}+24\sqrt{-3}q^{31}+6\sqrt{-6}q^{35}+\cdots, \end{aligned}$$

More concretely,

$$f(z)=\sum_{n\geq 1}c_p(f)q^n=f_1(12z)+6\sqrt{2}f_5(12z)+\sqrt{-3}f_7(12z)+6\sqrt{-6}f_{11}(12z), \tag{7}$$

where

$$f_1(z)=\frac{\eta(2z)^3\eta(3z)}{\eta(6z)\eta(z)}E_6(z),\qquad f_5(z)=\frac{\eta(z)\eta(2z)^3\eta(3z)^3}{\eta(6z)}$$
$$f_7(z)=\frac{\eta(6z)^3\eta(z)}{\eta(2z)\eta(3z)}E_6(z),\qquad f_{11}(z)=\frac{\eta(3z)\eta(z)^3\eta(6z)^3}{\eta(2z)}$$

where $E_6(z)=1+12\sum_{n\geq1}(\sigma(3n)-3\sigma(n))q^n$, and $\sigma(n)=\sum_{d|n}d$. Let ρ_f be Deligne's 2-dimensional λ-adic representation of $G_{\mathbb{Q}}$ attached to f, where λ is the place of $\mathbb{Q}_\ell(\sqrt{2},\sqrt{-3})$ lying over ℓ (see [Del68], [Lan72]). In particular the trace of arithmetic Frobenius Fr_p under ρ_f agrees with $c_p(f)$, the p-coefficient of f. These are the conventions of [DS75]. This is at variance with the conventions in [Del68] and in Scholl's papers, which match the characteristic polynomials of the geometric Frobenius with the Hecke polynomials Therefore we must take duals in the statement of our main results.

[2] Using the approach of [ALLL10], one can also derive that there exists a quadratic character ϕ of $G_{\mathbb{Q}(\sqrt{-3})}$ with fixed field $\mathbb{Q}(\sqrt[4]{-3})$ such that $(\sigma_{\lambda,2,-3}\otimes\psi\otimes\phi)^\vee=(\sigma_{\lambda,4,-3}\otimes\phi)^\vee$ agrees with $\rho_g|_{G_{\mathbb{Q}(\sqrt{-3})}}$ where ρ_g is the Deligne representation attached to a certain new form g, that is different from the new form f below.

We will now apply the method of Faltings-Serre (see [Ser84]) to prove the result below. Briefly, the idea is that given two nonisomorphic semisimple Galois representations $\rho_1, \rho_2 : G_K \to \mathrm{GL}_2(\mathbb{Q}_\ell)$ there is a finite list of $(\tilde{G}, t)$ that captures the difference between ρ_1, ρ_2, where each $\tilde{G}$ is a finite Galois group referred to as a *deviation group*, and $t : \tilde{G} \to \mathbb{F}_\ell$ is a function with certain properties that can be computed from ρ_1, ρ_2. To establish the isomorphism between the semisimplifications of ρ_1 and ρ_2 we need to eliminate each $(\tilde{G}, t)$ by explicit computation. The idea of the criterion is recast in [LLY05], right below the statement of Theorem 6.2.

Theorem 3. *Let $\sigma_{\lambda,4,-1}$ as before be the representation of $G_{\mathbb{Q}(i)}$ whose induction to $G_{\mathbb{Q}}$ is $\rho_{\ell,4} \otimes_{\mathbb{Q}_\ell} K_{-1,\lambda}$. There exists a quartic character χ of $G_{\mathbb{Q}(i)}$ which fixes $L = \mathbb{Q}(i, \sqrt[4]{3})$ such that up to semisimplification, $\rho_f \mid_{G_{\mathbb{Q}(i)}} \otimes \chi$ is isomorphic to $(\sigma_{\lambda,4,-1})^\vee$, the dual of $\sigma_{\lambda,4,-1}$, as $G_{\mathbb{Q}(i)}$ representations.*

Proof. The determinant $\det(\rho_f \mid_{G_{\mathbb{Q}(i)}} \otimes \chi) = \chi^2 \varepsilon^2 = \varphi_{-1} \varepsilon^2$, φ_{-1} is the quadratic character of $G_{\mathbb{Q}(i)}$ with kernel $G_{\mathbb{Q}(i,\sqrt{3})}$. It coincides with the determinant of $(\sigma_{\lambda,4,-1})^\vee$ by Corollary 1.

Let $H = G_{\mathbb{Q}(i)}$. By the explicit form of f, $\rho_f \mid_H$ is a 2-dimensional representation of H over $\mathbb{Q}_\ell(\sqrt{2})$. For any places v above $p \equiv 5 \mod 12$, the character χ takes values $\pm i$ and the characteristic polynomial of $\sigma_{\lambda,4,-1}(\mathrm{Frob}_v)$ is of the form $X^2 + a\sqrt{-2}X - p^2$ for some $a \in \mathbb{Z}$. For any places v above $p \equiv 1 \mod 12$, the character χ takes values ± 1 and the characteristic polynomial of $\sigma_{\lambda,4,-1}(\mathrm{Frob}_v)$ is of the form $X^2 + aX + p^2$ for some $a \in \mathbb{Z}$. Thus, the representation $\rho_f \mid_H \otimes \chi$ takes values in $\mathbb{Q}_\ell(\sqrt{-2})$, as does the representation $(\sigma_{\lambda,4,-1})^\vee$. In the proof below, we will see that it suffices to compare $c_p(f)\chi(v)$ with the trace of $\sigma_{\lambda,4,-1}(\mathrm{Frob}_v)$, that is, the trace of $(\sigma_{\lambda,4,-1})^\vee(\mathrm{Fr}_v)$ for every place v of $\mathbb{Q}(i)$ above the primes $p = 5$ and 13.

Now we can use Faltings-Serre modularity criterion effectively. We take the representation with coefficients in $\mathbb{Q}_2(\sqrt{-2})$. Let $\wp = (\sqrt{-2})$. We now consider both representations modulo $\wp$ with images in $\mathrm{SL}_2(\mathbb{F}_2)$. For simplicity, use $\bar{\rho}$ to denote $\overline{\rho}_{\ell,f}|_{G_{\mathbb{Q}(\sqrt{-1})}}$. The trace of $\bar{\rho}(\mathrm{Fr}_{2+3i}) = 1$ so the image has order 3 elements. If the image is C_3, then it gives rise to a cubic extension of $\mathbb{Q}(i)$ which is unramified outside of $1+i$ and 3. Like Lemma 19 of [Lon08], we know such a cubic field is the splitting field of $x^3 - 3x + 1$. It is irreducible mod $2+i$, but the characteristic polynomial of $\bar{\rho}(\mathrm{Fr}_{1+2i})$ is $T^2 + 1$, hence it is of order 1 or 2 which leads to a contradiction. So $\ker \bar{\rho}$ corresponds an S_3-extension of $\mathbb{Q}(i)$ which can be identified as the splitting field of $x^3 - 2$ over $\mathbb{Q}(i)$.

Now we are going to consider all possible deviation groups $\widetilde{G}$ measuring the difference between $(\sigma_{\lambda,4,-1})^\vee$ and $(\rho_f \mid_{G_{\mathbb{Q}(i)}}) \otimes \chi$ if they are not isomorphic up to semisimplification.

Let F' be the splitting field of $x^3 - 2$ over $\mathbb{Q}$. Similar to the proof of Lemma 19 of [Lon08], we first look for S_4-extensions L' of $\mathbb{Q}$ containing F' but not $\mathbb{Q}(i)$ and unramified outside of 2 and 3. By using the fact that their cubic resolvent is $x^3 - 2$ we conclude that such S_4 extensions are the splitting fields of irreducible polynomials of the form $x^4 + ux^2 + vx - u^2/12$ where $u, v \in \mathbb{Z}[1/6]$ such that $8u^3/27 + v^2 = \pm 2$. The possible polynomials giving non-isomorphic fields are

$$x^4 + 6x^2 + 8x - 3, \quad x^4 - 18x^2 + 40x - 27.$$

Fr_5 has order 4 in these fields. By comparing the traces of $\mathrm{Frob}_{1\pm 2i}$ (or $\mathrm{Fr}_{1\pm 2i}$) for both representations, we eliminate the possibility that $\widetilde{G}$ contains S_4 as a subgroup.

The remaining possibility is $\widetilde{G} = S_3 \times \mathbb{Z}/2$. Among all the quadratic extensions $\mathbb{Q}(i, \sqrt{d})$ of $\mathbb{Q}(i)$ unramified at $1+i$ and 3: $d = i, 1+i, 1-i, 3+3i, 3-3i$, we have that Fr_v for $v = 3+2i, 3+2i, 3-2i, 3+2i, 3-2i$ are inert in these fields respectively. Meanwhile these Frobenius elements map under $\bar{\rho}$ to an element of order 3. Such an element in the conjugacy class of Fr_v has order 6 as it has order 3 in the S_3 component and order 2 in the $\mathbb{Z}/2$ component. Since the characteristic polynomials of $\mathrm{Frob}_{3\pm 2i}$ (or $\mathrm{Fr}_{3\pm 2i}$) under both representations agree, we know $\widetilde{G}$ cannot be $S_3 \times \mathbb{Z}/2$ either, because if the two representations were different, they would have different traces at elements of order 4 or higher in the deviation group, see [LLY05]. □

Corollary 2.

$$L(s, \rho_{\ell,4}^{\vee}) = L(s, (\sigma_{\lambda,4,-1})^{\vee}) = L(s, \rho_f\ |_{G_{\mathbb{Q}(i)}} \otimes \chi)$$

where $\rho_f\ |_{G_{\mathbb{Q}(i)}} \otimes \chi$ is a $GL_2(\mathbb{A}_{\mathbb{Q}}) \times GL_2(\mathbb{A}_{\mathbb{Q}})$ and hence a $GL_4(\mathbb{A}_{\mathbb{Q}})$ automorphic form by a result of D. Ramakrishnan [Ram00].

6. Atkin-Swinnerton-Dyer congruences

6.1. Let $V_{p,a}$ be the 4-dimensional F-crystal ($\mathbb{Q}_p$ vector space with Frobenius action) associated with $S_3(\Gamma)$ in the model of the curve $X(\Gamma)$ with Hauptmodul r_a. Note that the only difference among the $V_{p,a}$ is the action of the Frobenius F. We need to consider both $a = 2, 4$: for $a = 4$ it is easier to describe the modularity of the ℓ-adic counterpart $\rho_{\ell,4}$ (see Theorem 3) and the factorization of $H_{p,4}(X)$, but to prove 3-term ASD congruences in the simplest form for the expansion coefficients of the cuspforms h_1, h_2 relative to the q-parameter via the results of Scholl's paper [Sch85i], [Sch85ii], we need $a = 2$. We could derive ASD congruences using the F-crystal $V_{p,4}$ but these would be expressed in a parameter γq for some algebraic number γ. Therefore we only consider the F-crystal $V_p = V_{p,2}$.

6.2. The method is the following. We use the operators B_s (resp. B_s^*) $s = -1, \pm 3$ to decompose both V_p (resp. $W_\ell := W_{\ell,2}$) into eigenspaces $V_{p,s}^{\pm}$ (resp. $W_{\lambda,s}^{\pm}$). By the way B_s are defined, we know that B_s is defined over the field $L_{-1} = \mathbb{Q}(i) \cdot \mathbb{Q}(\sqrt[3]{2})$, $L_{-3} = \mathbb{Q}(\sqrt{-3})$ and $L_3 = \mathbb{Q}(\sqrt{3}) \cdot \mathbb{Q}(\sqrt[3]{2})$ for $s = -1, -3, 3$ respectively (see §3.5). We show that for each prime $p \geq 5$ there is an s such that the Frobenius F acts on the 2-dimensional eigenspaces $V_{p,s}^{\pm}$ which corresponds to an Frob_p in G_{L_s} acting on $W_{\lambda,s}^{\pm}$. For $p \equiv 1 \bmod 3$ we use $s = -3$; for $p \equiv 5 \bmod 12$ we use $s = -1$; for $p \equiv 11 \bmod 12$ we use $s = 3$. Following the approach of Scholl [Sch85ii], there is a comparison theorem between Frobenius action on both ℓ-adic and p-adic spaces that implies

$$\mathrm{Char}(F, V_{p,s}^{\pm}, X) = \mathrm{Char}(\mathrm{Frob}_p, W_{\lambda,s}^{\pm}, X), \tag{8}$$

where the right hand side can be computed from f, ψ and χ. (Also the Frobenius Frob_p needs further justification to ensure it commutes with B_s^*.) In particular, for primes $p \equiv 2 \mod 3$, the right hand side can be computed from f and χ only by using Lemma 1. We find the ASD basis as linear combinations $h_1 \pm \alpha h_2$ which span the 1-dimensional spaces

$$V_p^{\pm} \cap (S_3(\Gamma) \otimes \overline{\mathbb{Q}}_p).$$

By the Cayley-Hamilton theorem, $\mathrm{Char}(F, V_p^{\pm}, F)(g) = 0$ for any $g \in V_p^{\pm}$. Writing out the Frobenius action in the local coordinate r_2 applied to the eigenfunctions $h_1 \pm \alpha h_2$, this gives the desired three term ASD congruences.

6.3. $p \equiv 1$ **mod** 3.

Proposition 4. *For every prime $p \equiv 1 \mod 3$, h_1, h_2 form a basis of $S_3(\Gamma)$ for the three-term ASD congruences at p given by the characteristic polynomial $X^2 - \tau_i(a_p)X + \tau_i(b_p)p^2 \in \mathbb{Q}_p[X]$ where $a_p, b_p \in \mathbb{Q}(\sqrt{-3})$, b_p a 6th root of unity, and τ_1, τ_2 are two different embeddings of $\mathbb{Q}(\sqrt{-3})$ into $\mathbb{Q}_p$. Moreover, a_p differs from the pth coefficients of f by at most a twelfth root of unity that can be determined by ψ and χ defined as before.*

Proof. Let $p \equiv 1 \mod 3$ be a prime. The cuspforms h_1 and h_2 are distinct eigenvectors the B_{-3}-operator. On W_ℓ, the corresponding operator B_{-3}^* is defined over $\mathbb{Q}(\sqrt{-3})$, hence commutes with Frob_p. Consequently,

$$H_{p,2}(X) = (X^2 - a_p X + b_p p^2)(X^2 - \bar{a}_p X + \bar{b}_p p^2)$$

for some $a_p, b_p \in \mathbb{Q}(\sqrt{-3})$ and the bar denotes complex conjugation. The value of b_p can be determined by Theorem 1 and Theorem 3. The claim follows from (8) and the discussion in the beginning of this section.

□

6.4. $p \equiv 2$ **mod** 3. In this case $X^3 - 2$ has exactly one root in $\mathbb{F}_p$ which gives rise to a unique embedding of $\mathbb{Q}(\sqrt[3]{2})$ in $\mathbb{Q}_p$. In the sequel, we regard $\sqrt[3]{2}$ as an element in $\mathbb{Q}_p$.

Proposition 5. *When $p \equiv 5 \mod 12$, let τ be an embedding of $\mathbb{Q}(i, \sqrt{2})$ to $\mathbb{Q}_p(\sqrt{2})$. The functions $h_1 \pm \frac{\tau(2^{1/2})}{2^{1/3}} h_2$ form a basis for the three-term ASD congruences at p given by the characteristic polynomial $X^2 \pm a_p \tau(\sqrt{-2})X - p^2 \in \mathbb{Q}_p(\sqrt{2})[X]$ where $a_p \in \mathbb{Z}$ and $a_p \cdot \sqrt{-2}$ differs from the pth coefficients of f by a fourth root of unity.*

Proof. Let $p \equiv 5 \mod 12$ be a prime. The operator B_{-1} is defined over the field $L_{-1} = \mathbb{Q}(\sqrt{-1}) \cdot \mathbb{Q}(\sqrt[3]{2})$. In the ring of integers of L_{-1} there is a unique place above p with relative degree 1. By abusing notation, we denote this place by p again. Under this assumption Frob_p commutes with B_{-1}. Thus Frob_p (as an element of $G_{L_{-1}}$) acts on the eigenspace $W_{\lambda,-1}^{\pm}$ and (8) holds. By Lemma 1,

$$\mathrm{Char}(F, V_{\lambda,-1}^{\pm}, X) = \mathrm{Char}(\mathrm{Frob}_p, W_{\lambda,2,-1}^{\pm}, X) = \mathrm{Char}(\mathrm{Frob}_p, W_{\lambda,4,-1}^{\pm}, X).$$

As a consequence of $\rho_{\ell,4}$ satisfying the quaternion multiplication, we know that

$$\mathrm{Char}(\mathrm{Frob}_p, W_{\lambda,4,-1}^{\pm}, X) = X^2 \pm a_p\sqrt{-2}X - p^2$$

for some $a_p \in \mathbb{Z}$. By Theorem 3, $a_p\sqrt{-2}$ is different from the pth coefficient of f by a 4th fourth root of unity as χ takes value $\pm i$ for any place v above $p \equiv 5 \mod 12$ in $\mathbb{Z}[i]$. The eigenfunctions of B_{-1} are $h_1 \pm \frac{2^{1/2}}{2^{1/3}} h_2$. For any embedding τ of $\mathbb{Q}(i, \sqrt{2})$ to $\mathbb{Q}_p(\sqrt{2})$, $h_1 \pm \frac{\tau(2^{1/2})}{2^{1/3}} h_2$ is a formal power series in $\mathbb{Q}_p(\sqrt{2})[[q]]$. It satisfies the three term ASD congruences at p given by $X^2 \pm \tau(a_p)X - p^2$ as claimed. □

Proposition 6. *When $p \equiv 11 \mod 12$, let τ be an embedding of $\mathbb{Q}(\sqrt{3}, \sqrt{-2})$ to $\mathbb{Q}_p(\sqrt{-2})$. The functions $h_1 \pm \frac{\tau((-2)^{1/2})}{2^{1/3}} h_2$ form a basis for the three-term ASD congruences at p given by the characteristic polynomial $X^2 \pm a_p \tau(\sqrt{-6})X - p^2 \in \mathbb{Q}_p[T]$ where $a_p \in \mathbb{Z}$ and $a_p\tau(\sqrt{-6})$ differs from the pth coefficients of f by at most a most a $\pm$ sign.*

Proof. The reasoning is similar to the previous case but with the operator B_3, defined over $\mathbb{Q}(\sqrt{3}) \cdot \mathbb{Q}(\sqrt[3]{2})$ with $B_3^2 = -24$. □

7. TABLES

In tables 1, 2 we display the factor $g_{p,a}(X)$ such that the characteristic polynomial of Frob_p is $H_{p,a}(X) = g_{p,a}(X)\overline{g_{p,a}(X)}$. When $a = 2$, we write this in the form

$$g_{p,2}(X) = X^2 - \zeta c_p(f)X + (-4/p)\zeta^2 p^2$$

for a twelfth root of unity ζ.

p	$g_{p,2}(X)$	$c_p(f)$	ζ
5	$X^2 + 6\sqrt{-2}X - 5^2$	$6\sqrt{2}$	i
7	$X^2 + \sqrt{-3}\left(\frac{-1-\sqrt{-3}}{2}\right)X - \left(\frac{-1+\sqrt{-3}}{2}\right)7^2$	$-\sqrt{-3}$	ω^4
11	$X^2 + 6\sqrt{-6}X - 11^2$	$-6\sqrt{-6}$	1
13	$X^2 - 13\left(\frac{1+\sqrt{-3}}{2}\right)X + \left(\frac{-1+\sqrt{-3}}{2}\right)13^2$	13	ω
17	$X^2 + 6\sqrt{-2}X - 17^2$	$-6\sqrt{2}$	i
19	$X^2 + 11\sqrt{-3}\left(\frac{-1+\sqrt{-3}}{2}\right)X - \left(\frac{-1-\sqrt{-3}}{2}\right)19^2$	$-11\sqrt{-3}$	ω^2
23	$X^2 - 18\sqrt{-6}X - 23^2$	$18\sqrt{-6}$	1
29	$X^2 + 24\sqrt{-2}X - 29^2$	$-24\sqrt{2}$	i
31	$X^2 - 24\sqrt{-3}X - 31^2$	$24\sqrt{-3}$	ω^6
37	$X^2 - 35\left(\frac{-1-\sqrt{-3}}{2}\right)X + \left(\frac{-1+\sqrt{-3}}{2}\right)37^2$	35	ω^4
41	$X^2 - 41^2$	0	i
43	$X^2 + 24\sqrt{-3}X - 43^2$	$-24\sqrt{-3}$	ω^6
47	$X^2 - 6\sqrt{-6}X - 47^2$	$6\sqrt{-6}$	1
53	$X^2 - 36\sqrt{-2}X - 53^2$	$36\sqrt{2}$	i
59	$X^2 - 30\sqrt{-6}X - 59^2$	$30\sqrt{-6}$	1

TABLE 1. Factorization of $H_{p,2} = g_{p,2}(X)\overline{g_{p,2}(X)}$, coefficients of f; $\omega = \exp(2\pi i/6)$, $i = \sqrt{-1}$.

REFERENCES

[ALLL10] A. O. L. Atkin, W. C. Li, T. Liu, and L. Long, *Galois representations with quaternion multiplications associated to noncongruence modular forms*, arXiv:1005.4105 (2010).

[ALL08] A. O. L. Atkin, W. C. Li, and L. Long, *On Atkin and Swinnerton-Dyer congruence relations (2)*, Math. Ann. **340** (2008), no. 2, 335–358.

[Cli37] A. H. Clifford, *Representations induced in an invariant subgroup*, Ann. of Math. (2) **38** (1937), no. 3, 533–550.

[DeRa] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques.* Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), pp. 143–316. Lecture Notes in Math., Vol. 349, Springer, Berlin, 1973.

[Del68] P. Deligne, *Formes modulaires et représentations l-adiques*, Sém. Bourbaki, 355, 139-172.

p	$g_{p,4}(X)$	$c_p(f)$
5	$X^2+6\sqrt{-2}X-5^2$	$6\sqrt{2}$
7	$X^2+\sqrt{-3}X-7^2$	$-\sqrt{-3}$
11	$X^2+6\sqrt{-6}X-11^2$	$-6\sqrt{-6}$
13	$X^2+13X+13^2$	13
17	$X^2+6\sqrt{-2}X-17^2$	$-6\sqrt{2}$
19	$X^2+11\sqrt{-3}X-19^2$	$-11\sqrt{-3}$
23	$X^2-18\sqrt{-6}X-23^2$	$18\sqrt{-6}$
29	$X^2+24\sqrt{-2}X-29^2$	$-24\sqrt{2}$
31	$X^2-24\sqrt{-3}X-31^2$	$24\sqrt{-3}$
37	$X^2-35X+37^2$	35
41	X^2-41^2	0
43	$X^2+24\sqrt{-3}X-43^2$	$-24\sqrt{-3}$
47	$X^2-6\sqrt{-6}X-47^2$	$6\sqrt{-6}$
53	$X^2-36\sqrt{-2}X-53^2$	$36\sqrt{2}$
59	$X^2-30\sqrt{-6}X-59^2$	$30\sqrt{-6}$

Table 2. Factorization of $H_{p,4}=g_{p,4}(X)\overline{g_{p,4}(X)}$, coefficients of f.

[DS75] P. Deligne and J.-P. Serre, *Formes modulaires de poids* 1. Ann. Sci. École Norm. Sup. (4) 7 (1974), 507-530 (1975).

[DS05] F. Diamond and J. Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005.

[FHL+08] L. Fang, J. W. Hoffman, B. Linowitz, A. Rupinski, and Verrill H., *Modular forms on noncongruence subgroups and Atkin-Swinnerton-Dyer relations*, Experimental Mathematics, **19** no. 1, (2010), 1-27.

[KM85] N. M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves.* Annals of Mathematics Studies, 108. Princeton University Press, Princeton, NJ, 1985.

[Lan72] R. P. Langlands, *Modular forms and ℓ-adic representations.* Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Lecture Notes in Math., Vol. 349, Springer, Berlin, 1973 pp. 361–500.

[LLY05] W. C. Li, L. Long, and Z. Yang, *On Atkin and Swinnerton-Dyer congruence relations*, J. of Number Theory **113** (2005), no. 1, 117–148.

[Lon08] L. Long, *On Atkin and Swinnerton-Dyer congruence relations (3)*, J. of Number Theory **128** (2008), no. 8, 2413–2429.

[Ram00] D. Ramakrishnan, *Modularity of the Rankin-Selberg L-series, and multiplicity one for* SL(2), Ann. of Math. (2) **152** (2000), no. 1, 45–111.

[Sch85i] A. J. Scholl, *A trace formula for F-crystals.* Invent. Math., **79** (1985), 31-48.

[Sch85ii] ——, *Modular forms and deRham cohomology; Atkin-Swinnerton-Dyer congruences.* Invent. Math., **79** (1985), 49-77.

[Sch90] ——, *Motives for modular forms.* Invent. Math. 100 (1990), no. 2, 419–430.

[Ser84] J.P. Serre, Résumé de cours, Collège de France 1984/5.

[Shi71] G. Shimura, *Introduction to the arithmetic theory of automorphic forms*, Iwanami Shoten and Princeton U. Press, 1971.

Department of Mathematics, Louisiana State University, Baton Rouge, LA 70803, USA

E-mail address: hoffman@math.lsu.edu

Department of Mathematics, Iowa State University, Ames, IA 50011, USA

E-mail address: linglong@iastate.edu

Warwick Mathematics Institute, UK

E-mail address: H.A.Verrill@warwick.ac.uk